An Access Control System to Improve Security Amongst Randomly Associated Nodes in BYOD Network.

A Thesis Submitted at the University of Bedfordshire

In partial fulfilment for the degree of

Masters of Science

In

Computer Security and Forensics

Francis Nwebonyi Nwebonyi

1029282

Supervisor: **Dr. Gregory Epiphaniou**

Department of Computer Science and Technology

University of Bedfordshire

May, 2013

ABSTRACT

The growth of mobile devices both in variety and in computational abilities have given birth to a concept in the corporate world known as Bring Your Own Device (BYOD). Employees are allowed under this concept to bring personally owned mobile devices for official work. Though relatively new, it has gained up to 53% patronage among organisations, and it is expected to hit 88% in the near future. Its popularity is driven by the significant advantages it brings along such as reduced cost, employee satisfaction and improved productivity, to mention a few. However, as a relatively new concept, it also introduces new security challenges; for instance, the organisation looses the ownership of devices used for official work, to the employees. Implying that the employees own and manage the devices they use to work, including seeing to the security needs of such devices. With this development, protecting the corporate network becomes more challenging; outsmarting the usual traditional access control mechanisms, owing to the highly dynamic nature of mobile devices. Considering the fact that BYOD is also a type of pervasive/dynamic environment, this work studies similar dynamic environments, relating to how their security challenges are addressed, as bases to propose an algorithm for enhancing the security of BYOD via access control. Various access control mechanisms have also been adequately analyzed as a justification for the proposed approach.

ACKNOWLEDGEMENT

I wish to specially acknowledge my supervisor Dr Gregory Epiphaniou for his sincere impartation of knowledge as my lecturer and as the overseer of this work. My thanks also goes to all my lecturers whose encouragements propel me into hard work towards the actualization of this project.

My appreciation goes to my parents Dr and Mrs Francis I. Nwebonyi, and to all my siblings especially Mr. Loius Nwebonyi for their ceaseless support and advice.

I am also grateful to Educational Trust Fund (ETF) and Ebonyi State University of Nigeria under the administration of Prof. F. I. Ididke, for an offer of sponsorship.

My gratitude also goes to all my friends especially; Odeyinka Olatunbosun, Abdulahi Jingi, Uchenna Ani, Elias Eze, and Paschaline Nwali, for their support throughout the period of this work.

DEDICATION

This project work is dedicated to Almighty God for his grace and mercy throughout the period of this study.

CONSENT FORM

Thesis author consent form

AUTHOR'S NAME: FRANCIS NWEBONYI NWEBONYI

TITLE OF THESIS: AN ACCESS CONTROL SYSTEM TO IMPROVE SECURITY AMONGST RANDOMLY ASSOCIATED NODES IN BYOD NETWORK.

DEGREE: MSc. COMPUTER SECURITY AND FORENSICS

Please read carefully and sign the following as appropriate.

I have read and understood the University's regulations and procedures concerning the submission of my thesis.

I understand that I have already signed a declaration agreeing to my dissertations being kept in the Learning Resources Centre (LRC) when I enrolled.

We would like now, to extend this agreement by making the thesis available online. Further to this,

I AGREE AS FOLLOWS:

- That I am the author of the work.

- That I have exercised reasonable care to ensure that the Work is original, and does not to the best of my knowledge break any UK law or infringe any third party's copyright or other Intellectual Property Right.

- The LRC and BREO administrators do not hold any obligation to take legal action on behalf of the Depositor (you), or other rights holders, in the event of breach of intellectual property rights, or any other right, in the material deposited.

1. I hereby extend my consent to this thesis being included in the LRC as well as on BREO via online access.

AUTHOR'S PERSONAL SIGNATURE:

AUTHOR'S STUDENT NUMBER: 1029282

DATE 24TH May 2013

Table of Contents

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE

INTRODUCTION

Bring Your Own Device (BYOD) is a concept that allow employees to bring personally owned mobile devices for official work. It has gained much popularity among enterprises because of the tremendous growth in the number of mobile devices available in the market today. The concept is bringing a shift from the usual approach where concerned organisations/enterprises usually own and manage the devices used for official tasks. In such traditional network settings, the organisation owned it all, and has fewer worries about what connects to their network since the IT department knows about all the devices, and checks them for security compliance. BYOD shifts the ownership of these devices to the employees, and introduces mobile devices instead of the relatively stationary ones. Its advantages are very pronounced, some of which includes (i) saving the cost of purchasing and maintaining organisational devices, (ii) more employee satisfaction, and (iii) increased productivity and efficiency (Mansfield-Devine, 2012).

Despite the all-interesting advantages of BYOD, it comes along with some security concerns that demand the attention of not just organisations but researchers as well. Access control have been identified as a vital security approach in ensuring the security of corporate network resources. Unfortunately, the traditional access control mechanisms such as Role Based Access Control (RBAC), Discretionary Access Control (DAC) and Mandatory Access Control (MAC) used in traditional network systems are inadequate for the dynamic nature of mobile devices involved in BYOD; owing to their bases on the identity/role of users, which are reasonably static (Sun&Denko, 2008). Other non discretionary access control systems have also emerged, and have been specifically channelled to various particular pervasive/dynamic environments with result. Nevertheless, as discussed in the next chapter, these approaches are not adequate for BYOD type of pervasiveness/dynamism.

In many pervasive environments however, Trust have played vital roles in making access control systems more dynamic by allowing the use of dynamic features (or attributes) for access permission decision, similar to the natural way the human society handle security.

Following the testimonies of trust in other pervasive/dynamic environments, we introduce its concept into the access control system of BYOD network (Lagesse et al., 2009) (Lee, Kim & Hong, 2008). The trust value will be assigned to individual nodes for the first time, based on some characteristics of the device and its registration status, in compliance with the organisational policy. It shall then be regularly updated after each interaction to reflect their current security status, as a means of identifying malicious nodes dynamically.

The proposed algorithm will receive updates from an assumed intelligent system concerning the behaviour of interacting nodes. Such information will be used to update the behavioural history, and subsequently used for the calculation of trust value in order to predict beforehand if a node is of malicious intent or potentially safe. Access is granted to only potentially safe nodes. We take a standpoint where concerned organisations' policy will contain a provision for the minimum threshold for accessing the network resources, while the trust engine assigns a trust value to first time devices and regularly updates the interaction history of each node. Our approach shall be mathematically backed using probability concepts which have been shown to be efficient in trust management (Ping&Jing, 2007).

1.1 Aim and Objectives

The aim of this work is to derive an algorithm for a device aware access control system that increases the security BYOD networks based on trust. The algorithm is to ascertain the trust worthiness of interacting nodes beforehand via trust value computation, which is then used for access permission decision. This is geared towards securing the network resources by dictating and dropping malicious (non trustworthy) node(s) out of the network to prevent it from causing security breaches. The past behaviour of devices will be used to infer the next behaviour when it connects to the network, in order to determine if it merits a pass to the network resources or otherwise.

The following objectives shall be achieved;

- Extensive review of existing access control and trust models.
- Deriving suitable parameters for acquiring and monitoring interaction history of the randomly associated nodes.

- Deriving a mathematical method of computing trust value of nodes, which also portray their expected behaviour if allowed access to the network.
- Proposing a trust based algorithm for screening out malicious nodes in a BYOD network, as a way of increasing its security. The past interactions of each randomly associated node will be used to calculate its subsequent security behaviour using the principles of probability theory.

1.2 Problem Statement

BYOD as a type of pervasive environment involves unavoidable mutual collaborations of mobile devices, leading to more security issues than those experienced in traditional networks (Mohammed, 2008). The IT department of the organisations involved cannot answer questions concerning the security state of the interacting nodes at any point, because the ownership of the devices have been lost to the employees. Similar, the shift to mobile devices, as against the relatively stationary ones used in traditional network systems also comes with fresh challenges. For instance, mobile devices easily collaborate with other devices outside the organisational network, thus exposing it to a higher risk of threat, and making it more difficult to securely incorporate them into a network.

Traditional access control systems are therefore not adequate for the dynamic and mobile nature of the involved devices, since they only base permission decisions on user identity or role(s) (Sun&Denko, 2008). Other approaches as shall be reviewed in the next chapter are either not dynamic enough to keep track of these mobile devices as they roam in and out of compliance, or are specifically channelled for specific environments and therefore cannot fit into the security needs of BYOD. There is therefore the need for a more sensitive and automatic means of watching the behaviour of interacting nodes, minding the fact that it is no longer feasible to go round physically, to check for security compliance of devices.

Accordingly, we propose an algorithm that can automatically check the security compliance of each randomly associated nodes at access point; allowing only the nodes that are considered safe to access the network. This enhances the security of the network by protecting it from threats that may originate from malicious nodes. The algorithm is based on the concept of trust. The behaviour of interacting nodes will be monitored and updated

regularly to detect when a device fall out of compliance. Through this means, maliciously behaving nodes will be dropped out, to prevent it from causing havoc on the entire network.

1.3 Motivation of Study

The concept of BYOD is becoming prevalent, and many organisations are shifting towards it. The recent research of (Ghosh, Gajar & Rai, 2013) reveal that 53% of corporate organisations have endorsed the concept of BYOD and had already begun its use. The authors described it as a brand new concept, yet it has gained this level of popularity, we anticipate that in the near future it will spread significantly wider to many more organisations. This tremendous growth is emphasised in (Scarfo, 2012), where 88% of IT leaders have been presented as seeing a future in BYOD.

As we know, the concept massively involves mobile devices; owned and looked after by employees. Sadly, users of mobile devices are usual careless about security issues; up to 66% of them never uses any form of antivirus or security applications to guard against compromise (Zineddine&Kindi, 2012). This makes it rather risky for any organisation to rely on users (employees) for the security of their network.

Awareness alone cannot solve this problem, the hands of researchers therefore needs to be on deck, in order to achieve secure BYOD network. In response to this therefore we employ the concept of trust which has been applied in other specific pervasive environments into the concept, as a way of dynamically dictating and sieving out malicious nodes from the network to enhance security. This would save the numerous organisations trooping into the idea, from huge potential loss, knowing that even a single malicious node could jeopardize the entire network leading to loss of vital organisational resources.

1.4 Scope and Limitation

The limitations of the scope of study are as follows;

- Although BYOD majorly involves the employees of organisations as pointed out earlier, there could also be a possibility of the need for a non-employee to officially

access the corporate network with a device that may not be registered. Such provision would require a form of recommendation, and have not been addressed in this work due to study and time constraints.

- The proposed approach is also based on an assumed intelligent system from where it fetches the behaviour information of the randomly associated nodes to update the interaction history accordingly. This is a limitation because without such system in-place the proposed algorithm may not function adequately.

- This work has not covered the implementation of the algorithm on a real time network or into full grown software.

- Finally, the algorithm is based on probability concepts, and thus may not prove 100% in all occasions at all times.

1.5 Outline of the Study

This work is arranged in four chapters as follows;

Chapter one presents a general overview of the work. The aims and objectives were adequately highlighted to give an insight on the project. This was followed by the motivation for the research, and subsequently, the scope and limitation of study.

Chapter two reviews the related literature. Accordingly, specific literatures on BYOD were first presented, revealing the current face of the concept. Access control systems were also reviewed to give due justification of the proposed algorithm. Also presented in the chapter includes trust concept and its important place in security considerations. We also reviewed specific pervasive environments where trust have been successfully proposed and/or applied, as a motivation for the proposed approach.

Chapter three presents the proposed algorithm, starting with explanation on the basic concepts. It covers some inherited concepts from the reviewed approaches. The flowchart of the algorithm is also presented here with the explanation of the steps, and the pseudo code.

The mathematical model which forms the basis for the algorithm is also discussed and used for sample calculations to buttress its relevance. A comparison is presented between the proposed system and the already in-place approach, which illustrated the relevance of the new approach.

Chapter four then presents the conclusion of the study and recommends areas of development and future work.

CHAPTER TWO

LITERATURE REVIEW

To address our objectives creditably, we shall review previous works on Bring Your Own Device (BYOD), Access Control Systems, existing trust models for pervasive environments, and general trust concepts.

2.1 Bring Your Own Device (BYOD)

BYOD though a new trend have attracted the attention of researchers in their reasonable number (Singh, 2012). The additional security loopholes created by the involved mobile devices must have been one of the major factors behind this increased research interest in the area. Such loopholes arise due to the mobility state and limited resources of the devices, which make them more prone to attack. The author of (Scarfo, 2012) placed these attacks under four major classes, maintaining that users also constitute attack vectors, since majority of them are not able to use common security mechanisms. He argued that any network system which entrusts reasonable security responsibilities on the employees (users) need to ensure adequate approaches to fend for potential threats that may arise even from the users.

Similarly, a research work (Furtmüller, 2013) was dedicated to the challenges arising from mobile devices, particularly in BYOD. The challenges were classified as follow; Physical risk (resulting from theft of devices), Access risk (resulting from uncontrolled access by devices), usage risk (as a result of collaboration with other devices and applications) and memory risk (acknowledging the limited resources of mobile devices). Earlier before Furtmuller's work, in (Mobileiron, 2011), it was identified that trust is strategic in addressing the challenges of BYOD based network. They pointed out that mobile devices are dynamic in nature and as such demands a dynamic approach to monitor them as they roam in and out of compliance. In our work, we capitalise on trust to derive an access control algorithm through which some or most of the problems identified above would be addressed, specifically the Access risk.

The authors in (Armando et al., 2013) worried about the wide gap between computational capabilities of mobile devices and the security provisions in their operating systems, stressing

that a good number of security breaches arise from some malicious applications which the users may install. They therefore proposed a BYOD security framework to sieve applications that users can install on their devices, and by that means forbid any application that does not comply to the security requirements from being installed. Though a commendable improvement from earlier works that just suggested the problems, it has a weak point, minding the fact that all the threats encountered by mobile devices are not as a result of installing applications that are known to be malicious. Mere engagement of the device in some form of collaboration with other devices can get it infected with malware and viruses, which could even be more dangerous than known malicious applications. Therefore their system tend to proffer partial solution to the alarming security concerns.

Our method aims at monitoring the devices as they interact with the network, to infer malicious behaviour from past interactions, and to drop any suspected device. The benefit of this, is that it will mandate the users to follow the organisations' security policies not only by avoiding malicious applications as suggested in the previous approach, but also by installing recommended software such as antivirus and anti malware applications as a way of protecting their devices from threats. This method of dynamically checking the trustworthiness of devices have not been found in traditional access control systems and some other approaches that have been proposed for various pervasive environments, as further discussed subsequently.

2.2 Access Control Systems

The main function of access control is to regulate access to system resources and to mitigate related vulnerabilities. There are various access rights that could be granted to a user, such as read, write, execute, among others. Access Control Systems are classified into discretionary, mandatory and non-discretionary (popularized by Role Based). The traditional access control systems; Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role Based Access Control (RBAC) respectively falls into each of these classifications. However, none of these have proved competent in meeting up with the security requirements of dynamic/pervasive network environments, owing to their more stationary mode of operation as discussed in the following subsections (Park, Han & Chung, 2006).

2.2.1 Identity Based Access Control Systems

I. Discretionary Access Control (DAC); grants access to resources based on users' identity. It is discretional in the sense that it allows a user to extend access permission to other users, for instance; the windows operating system. With this system, the object owners have authority to determine what subject can gain access to a given object. DAC often involve the use of Access Control List (ACL) which specifies different objects, subjects and access privileges relating to them as shown in table 2.1. Many operating system available today uses DAC because of the provision for the owner of the object to make some changes in the access control; that is granting some other users access to the system (Yuan&Tong, 2005). The problem with this method is that it could lead to unintended changes that could affect the security of the system. Many organisations do not use DAC, since it does not offer robust protection as MAC and others. Additionally it is unfit for dynamic system because it is considerably static in operation.

Table 2.1: Access Control List (ACL)

Subject	Object i	Object ii	Object iii
	Salary File	Benefits File	Evaluation Process
Mr A	Read	Read/Write	None
Mr B	None	Read	None
Salary Program	Read/Write	Read	Execute

II. Mandatory Access Control (MAC); restricts access to resources based on strictly specified attributes or labels; no user (resource owner) has the right to grant access to others. The attributes used for access permission decisions are statically determined by the underlying policy. The level of clearance (authorisation) depends on the sensitivity of the object in question. Since it is mostly used in the military, some classifications that could be given to objects include; confidential, secret, among others. A subject with the authorization to access secret objects can also access lower objects such as confidential. But subjects with authorization to access confidential

objects cannot access the object classified as secret. MAC uses the references monitor usually implemented in the application kernel. Every access request must go through the reference monitor where the object classifications and the subject clearances are specified. A customized operating system is usually required for the reference monitor. The strong advantage of this approach is that it enforces all requests and cannot be easily by past (Chin&Older, 2010). It however has some major drawbacks, besides not being dynamic enough for pervasive/dynamic environments, the fact that a customized operating system is required for the reference monitor turns organisation off from its use.

III. Non Discretionary Access Control: the most popularly adopted form of non discretionary access control system is the Role Based Access Control (RBAC). In this case, the access right of the subject is dependent on their role. As opposed to direct attachment of authorisation to individuals, three layers are introduced between the subjects and the objects. They include; roles, procedures and sometimes data types. When a user is assigned a role, it means that he/she can perform the procedures which are under the definition of such role. Data types also relate to the objects through some procedures that are peculiar to it.

As a security measure, the least privilege idea is adopted, in which allow only the necessary roles to be activated for the user. The provision for role hierarchies and separation of duties makes RBAC organisation friendly. Role hierarchy allows a senior staff to inherit roles of the junior, just as the case could be in traditional organisational setting. RBAC is very suitable for many organisational security setting, which is also why it is considered most suitable for organisations compared to MAC and DAC. The basic rules of RBAC include (Ferraiolo&Kuhn, 2009):

- Assignment of Roles: subjects are only authorised for any transaction if there are roles assigned to them.

  That is: $\forall$ s,t, (exec(s,t) $\Rightarrow$ AR(s) $\neq \varnothing$

  Where s = subject, t = transaction, AR = Active Roles

- Role Authorization (RA): only the roles that have been approved for the subject can come up active. This is a way of preventing users from taking up unauthorized roles.

  That is: $\forall s, (AR(s) \subseteq RA(s))$

- Transaction Authorization (TA): only the transactions that are authorized for the active roles of the user can be executed.

  That is: $\forall$s,t, (exec(s,t) $\Rightarrow$ t $\in$ TA(AR(s))).

  Where the earlier defined parameters remain the same, and exec = execute.

As can be deduced so far, RBAC and other traditional access control systems (MAC and DAC) are not optimally dynamic and therefore have proved inadequate in meeting up with the security requirements of dynamic/pervasive network environments (Park, Han & Chung, 2006), (Yuan&Tong, 2005), owing to their more stationary mode of operation. Users' access rights are usually statically pre-computed; meaning that if there should be any changes to the access permission status of any user, then such changes can only be effected manually.

As a result of these inadequacies, alternatives have always been sought and various approaches have been proposed by scholars, which also fall under the non discretional class as discussed subsequently.

2.2.2 Other Non-Discretionary Access Control Systems

Here we discuss some of the access control systems that have emerged due to the inadequacies of the earlier discussed traditional access control system.

I. Attribute Based Access Control (ABAC): In ((Yuan&Tong, 2005), ABAC was proposed to ascertain the attribute of users as bases for allowing or disallowing access to system resources. Trust was later introduced into ABAC as presented in ((Lee, Kim & Hong, 2008), the authors presented trust as a core security tool, and further argued that the earlier models relied on certification from central servers, which are relatively static. Their approach was later channelled specifically to Grid system by the authors

of ((Lang et al., 2009), according to them Grid system is made up of several independent domains with a dynamic relationship between resources and the users, making identity based access control systems insufficient for the needed security requirement. The approach was redefined by (Jin, Krishnan & Sandhu, 2012) to cover the attributes of traditional access control systems; DAC, MAC and RBAC, as way of making it more unified.

With these improvements made on attribute access control systems, it is still limited in our view. For instance, none of the versions considered the status of the devices, but seem to focus every attention on just the users. We argue that in the case of mobile devices which roam in and out of compliance due to easy engagement in collaboration with other devices, considering the users only in access permission decision is not enough to guarantee a safe network. The devices being used demands similar measure of attention for a balanced security to be attained.

II. Risk-Aware RBAC: having identified Role Based Access Control as the most favourable of the traditional access control systems due to its organisation friendliness and cost effectiveness, authors in (Bijon, Krishnan & Sandhu, 2012) proposed a risk-aware RBAC in which the access permission decision is based on estimated risk, as opposed to the traditional RBAC system where access permission decision is based on pre-computed policies which returns same result always. This difference makes the new system dynamic in nature. A session risk threshold is used to check the number of roles that could be activated by any user at any given time, so as to keep watch at the level of damage that could be caused on the network assuming the user begins to act malicious. As shown in figure 2.1, their model is made up of Policy Enforcement Point (PEP), Policy Information Point (PIP), and Policy Decision Point (PDP) were employed to achieve their goal.

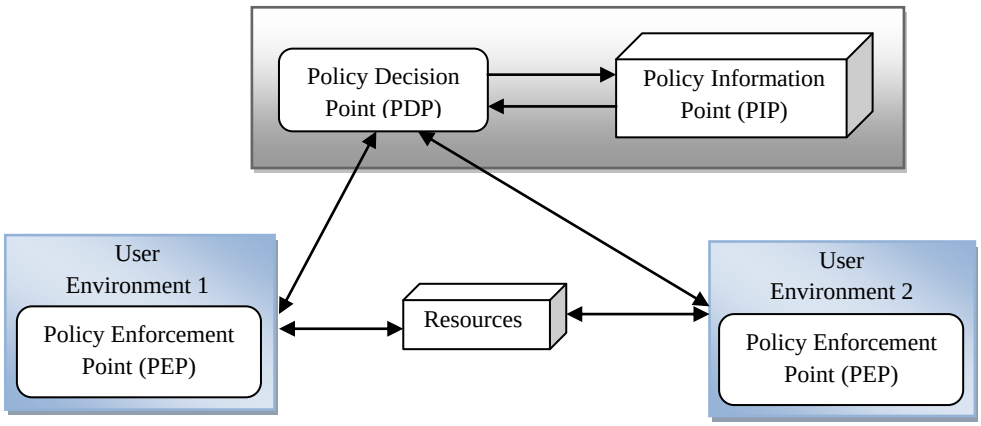


Figure 2.1: Risk Aware Access Control Model (Bijon, Krishnan & Sandhu, 2012)

The model unveiled a system that monitor the activities of users during any session, detecting malicious interactions or activities and preventing such malicious activities from continual occurrence within an active session time. Different risk levels were attached to different users, and the number of roles activated is not allowed to exceed the risk threshold. In their approach, an intelligent agent monitors the interaction of users and updates the system on interactions and triggers off when the risk threshold is exceeded within the session.

Though not trust based, their approach has particularly been reviewed here because of its highly dynamic nature and the fact that they share closely related ideas with the proposed system. Such ideas include dynamically eliminating malicious nodes from the network based on a threshold, to save it from further potential harm. Nevertheless, there are some problems with their system. For instance, their approach is only reactive and not proactive, in the sense that it can only stop already started malicious activity from continuing, but has no provision for preventing such threat from reoccurring. Similarly, only users are considered, without attention to the devices being used; ignoring the fact that a good number of threat can originate from devices rather than just users. We borrow the idea of intelligent agent monitoring the system and introduce the concept of trust to address the identified week points.

A close look at these approaches however, reveals that none of them is adequate for BYOD kind of pervasiveness. Apart from the traditional access control models which is strictly based on the identity or roles of users, and are static in operation as pointed out earlier, the

attribute based systems only emphasis on the users, and nothing about the device being used. This could mean that a compromised node can access the network without any form of check; thus exposing the entire network to potential jeopardize. The attributes used for access permission does not suit BYOD type of pervasive environment.

The risk based approach is considerable dynamic but it is only reactive and not proactive; meaning that it does not relate to the current behaviour of users to stop them from causing harm in the future. It only works for current sessions, added to the fact that emphasis are also on users only.

2.3 Trust in other Pervasive Environments

In this section, we shall highlight some specific pervasive environments where trust have been particularly channelled to meet their security needs. The testimonies of its success in these areas and more, motivates our study.

I. E-commerce as a kind of pervasive environment has gained particular attention from researchers, in-terms of trust application. This is evident in (Jøsang, Ismail & Boyd, 2007) where the authors identified reputation as very vital in fostering good behaviour and also encourages compliance to contract agreements in e-commerce. Similar to the real life scenario that would require some form of enforcement to foster compliance, their system introduced reputation system as a way of promoting adherence to electronic based agreements or contract, and encouraging trust in e-commerce, even among strangers. They argued that without such means as theirs, which uses past partner transaction experience to project into the future, there would be more tendencies to act in a deceptive manner for dubious gain during e-commerce transaction involving strangers. The trust management model presented in (Sun & Denko, 2008) also suits this scenario, with emphasis on how recommendations can be obtained and validated. Although their system considered the interacting devices, the specific requirements of BYOD were not its focal point and may not be adequately suitable.

II. Vehicular network is another specific pervasive environment where trust have been dedicatedly proposed for access control and enhanced security, the Situation Aware Trust (SAT) model proposed in (Hong et al., 2008) provides for building trust among vehicles in a network. They introduced the concept of social network as a means of ensuring trust decentralization even if the vehicular network is temporarily unavailable or is facing attack. Among the novelties they introduced includes incorporating the prediction of future trust conditions into the VNET, and linking the concept of trust from the normal social internet communities to vehicular network applications.

III. Social Networks: trust have also been introduced into online social networks as discussed in (Cutillo, Molva & Strufe, 2009)**,** they suggested that the real life view of trust can be employed towards a more secure online social network, and based on this to propose a system referred to as Safebook. They presented online social network as a digital reflection of the physical relationship that exist among participants. Acquiring genuine recommendations when the need arises was also been suggested in (Shuai et al., 2010). This cannot be suitable in a BYOD environment because their requirements are different from that of a mere social network.

IV. Professional Virtual communities: this an offshoot of social groups and online meeting, that provides a platform for professional knowledge sharing without face to face contact or meeting. The authors in (Hsu et al., 2007) identified that individuals not being willing to shear their knowledge is a major factor in VCs, and this willingness is a subject of expected outcome which is dependent on trust. Expected outcome in this context has to do with monetary gains or opportunities of interest which the user can trust the other party for before sharing needed information. They presented trust as an implication of a belief that a second party will act as expected, and argued that since there are lacks of physical interactions and legal guarantees in VCs, only a trust based model can be adequate. The representation of the model as shown in the figure 2.2, demonstrates the relationship that exist between trust and the processes of knowledge sharing.

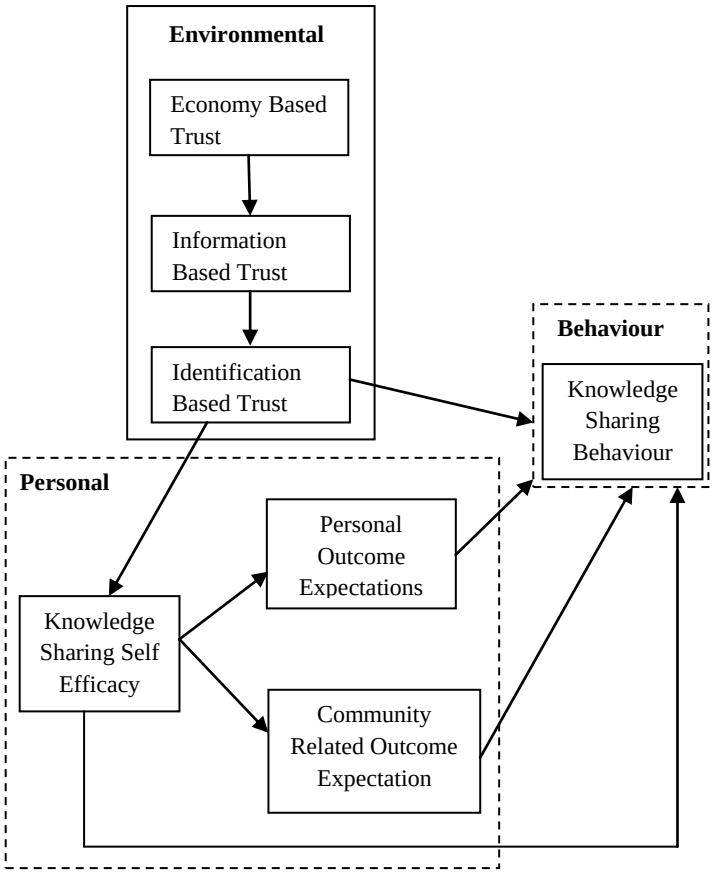


Figure 2.2: Trust in VC Environment (Hsu et al., 2007)

In each of these areas, specific emphasis has been laid on the specific needs of each of them, and so they cannot adequately suit the security needs of BYOD.

In line with our review so far, the authors of (Mármol&Pérez, 2009) identified that in many pervasive environments, the client nodes are usually the ones in need of acquiring the credibility/trust-worthiness of the server nodes. That is, the clients evaluating which service provider to trust and transact with. This is not exactly the same with BYOD, as the client nodes already have a reasonable trust on the corporate network (server). Our approach therefore presents a slight reverse of this usual pervasiveness, by introducing a way of enabling the corporate server in a BYOD environment to ascertain the trust worthiness of any client node before unleashing service(s) to them.

Furthermore, we centre on the behaviour of the devices, rather than just the users of the device; as seen in most of the earlier models. And we use the behaviour of each randomly

associated node to prevent potential occurrences of security breach instead of just reacting to current session as some of the approach discussed above suggests. Following the success story of trust in the discussed specific pervasive environments, we are certain that channelling trust to the specific need of BYOD will amount to a clearly more secure network implementation involving its randomly associated nodes.

We agree with the triple space of trust as presented in (Josang, 2001), which includes belief (favourable outcome), disbelief (unfavourable outcome) and uncertainty (not enough grounds to decide). Though their approach does not suit our scenario, as discussed previously, we adopted their idea of not specifying exactly 1 and 0 as values for passing and dropping a node respectively, instead we used a continuous real number range from 0 to 1, with specific specification on minimum threshold. This allows for devices to be granted access even without an absolute trust value of 1, provided the threshold is attained; since no device can be 100% trusted. We also adopted the ideas in (Wang et al., 2010) which include; effect of evidence and effect of conflict in the computation of the expected trust values of each returning randomly associated node. Effect of evidence: suggest that an increase in evidence result to an increase in certainty of trust, while the effect of conflict suggests that conflict in an evidence decreases certainty of trust. In our approach, the favourable behaviour of any randomly associated node represents the 'effect of evidence', while malicious behaviour of such nodes denotes the 'effect of conflict'.

In (Ping&Jing, 2007) and (Sun&Denko, 2008), the alpha beta probability concept have been presented as a competent means of predicting future occurrences from past experiences. We agree with their injunction and base our idea on the beta distribution as expressed as follows:

$$f(p|\alpha,\beta) = \frac{\gamma(\alpha+\beta)}{\gamma(\alpha)\gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1} \quad (1)$$

Where $0 \leq p \leq 1$, $\alpha > 0$, and $\beta > 0$.

With the constraint of the probability variable (p) not being 0 ($p \neq 0$) or being 1 ($p \neq 1$) when $\alpha < 1$ or $\beta < 1$ respectively, the expression for deriving the expected value of beta distribution from the known value is given as;

$$E(p) = \frac{\alpha}{\alpha + \beta} \quad (2)$$

As expressed in the next chapter, we redefined $\alpha \, and \, \beta$ to suit the requirements of our system without actually violating any mathematical injunctions.

2.4 General Trust Concepts

Having reviewed various applications of trust, it is worthwhile to quickly have a look at the concept of trust itself, as presented in this section.

Trust is inevitable in human life. We do most of our activities based on trust, for instance, getting on a bus and trusting the driver not to run into other cars on the road, driving our own cars trusting that they are safe enough for us, and trusting that that our money is safe in the bank, among others. It has also been identified as an inevitable concept in security, without which adequate reasoning of the security of any system may not be possible. (Giorgini, Mouratidis & Zannone, 2006). Despite this crucial importance of trust and its obvious application in our everyday lives, its definite meaning or definition is not always straight forward. Thus there is no agreement in its definition; different scholars view trust differently.

Trust could be viewed in terms of certainty and believe. This is to say that if Bob trust Alice, then it implies that Bob believes that Alice is trustworthy. If a device in a network trusts another device for an interaction, it is a reflection of this human attribute (believe) that the device will not act maliciously in a way that could cause security breach. It has been strongly suggested that trust grows in proportional measure to the amount of available evidence. This is to say that trust is based on evidence of favourable experiences with a given agent. Trust also grow with time, as the number of interaction with a given device increases, more

information about the device is gathered as bases for a clearer trust decision (Wang&Singh, 2007). Contrary to the effects of favourable evidences, unfavourable ones can also destroy trust believe. For instance if a device is used to acting behaviourally well, and suddenly begin acting maliciously, the earlier built trust may be reversed and such devices may not be trusted anymore. This attribute of trust is referred to as dynamism.

It can also be viewed in-terms of probability. In (Jøsang, 2001) a direct link was established between trust and the probability of outcomes; implying that the past behavioural history of users could be used to calculate the probability of their next behaviour. Favourable past behavioural history will suggest a trust, otherwise mistrust.

For the purpose of this study, we shall go in line with (Gambetta, 2000), in which trust was expressed in-terms of probability threshold. According to the author, trust refers to a level of probability in which a party bases his/her assessment that another party will act in a particular manner, usually before monitoring such action, and in a manner that defines his/her own action. The author first introduced probability range of 0 to 1, as representation of trust; with 0 representing mistrust and 1 representing absolute trust. He further explained that for a person to trust another, it means that there is high enough probability that the second party will act in a favourable manner or at least in a manner that will not be harmful. The proposed algorithm closely relates to this in finding out beforehand whether a node will act malicious or not if allowed access into the network, and with such information determine if access will be grated or not.

2.4.1 Forms of Trust

Apart from various formal definitions of trust, it has always been linked to some other aspects such as cooperation, commodity, and ethics, among others. We point out some of such relationships in this section, to buttress the importance of trust in our everyday lives, even in technology.

I. Trust In Relation To Cooperation

Gambetta in (Gambetta, 2000a) pointed out that without a reasonable level of trust; there will be no cooperation between involved agents. In that sense, he established a direct relationship between trust and cooperation. The chance of cooperation is usually higher if the trust level is high enough. The type of cooperation that we are considering in a BYOD network is the kinds that exist between the involved randomly associated nodes and the organisations' server. We relate to this relationship of trust, and suggest a kind of cooperation in which only trusted (safe) nodes are allowed to access the network.

II. Trust In Relation To Commodity

Although trust cannot be measured in unit like some other commodities, some scholars have also viewed it as a commodity and which can be measured. Reputation has always been pointed out as a clear basis for trust and one could say that they determine the extent (measurement) of trust. We relate to this reputation in our work; the history of node as they interact with the network reflects their reputation. The authors in(Parno, McCune & Perrig, 2010) emphasises this, and further relates trust to commodities such as computers.

2.4.2 Direct and Recommended Trust

Although we are limiting this work in the mean time to direct trust in order to allow for more elaborate work within the time frame, we shall also briefly discuss in this section the recommended trust. Direct trust is a kind of trust developed directly with an agent; usually as a result of past experiences (in this case it is a kind of employee/employer scenario; where some of employee's information is already known). While the recommended trust usually involve a party that have not been directly interacted with in the past, and there is no bases for trust. In such case the opinion of a third party is usually sort, as a way of asking if such party or agent is trustworthy. The responses from third parties are then used as a determinant for engaging or disengaging in any transaction with the agent (Lamsal, 2001).

Both direct and recommended trust can apply in BYOD network; the direct trust which we are considering entails a prior registration of employees' mobile devices as part of the criteria for first decision on trust concerning nodes joining the network for the first time. However there is also the possibility of unregistered device(s) legitimately accessing the network, in such case, we hope in the future to include a recommendation scenario where, the trust engine will allow for recommendation from the department where such device is connecting from; for trust decision making. The figure below illustrates direct and recommended trust;

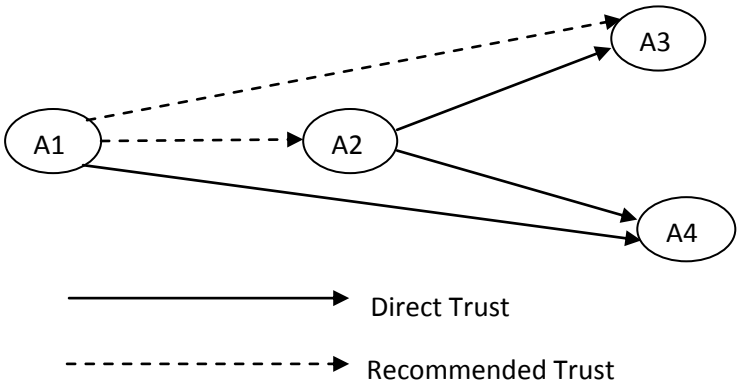


Fig 2.3; Direct and Recommended Trust

Figure 2.3 shows how direct trust can be extended among agents who are involved in interactions. A2 trusts A3 and A4, while A4 trusts A1. A1 has no trust relationship with A2 and A3 before, but as can be seen from the diagram, they now share recommended trust relationship. A4 recommended A1 for A2, while A2 further recommends it to A3.

2.5 Summary

From the works reviewed in this chapter, it could be observed that the concept of BYOD has come to stay. While its security limitations pose a source of worry to both the experts and organisations, its advantages constitute a strong driving force; giving it a firm stand in corporate organisations. Trust has also been presented to have seen high patronage in tackling security problems especially in dynamic and pervasive environments. The chapter have

addressed in detail the concepts of trust and how it will be applied in the proposed system based on alpha beta probability. The proposed algorithm is introduced in the next chapter.

CHAPTER THREE

3.0 PROPOSED ALGORITHM FOR A DYNAMIC ACCESS CONTROL SYSTEM FOR BYOD NETWORK; BASED ON TRUST

Probability Density Function (PDF) provides for inferring the future actions of individuals from their past interactions. This has seen huge patronage in various dynamic environments, especially in e-commerce. We relate to this, to infer the possibility of safe or unsafe interactions of BYOD nodes. The possibility of safe interaction is termed trust, while the possibility of unsafe interaction is tagged mistrust. The algorithm introduced in this chapter outlines how this can be applied to prevent potentially malicious (mistrusted) nodes from accessing the network, while allowing only the potentially safe (trusted) nodes. Through this means, the network can be kept free from threats originating from malicious devices; thus adding to the security level of the network.

Adequate network security may be difficult (if not impossible) to achieve without suitable access control system. It is a core security need because if access is not restricted in any way, then any user through any means can exploit the system. With this in mind, the proposed algorithm relates to the always available, traditional and human way of access control; trust, to introduce adequately dynamic access control approach for organisational networks which are BYOD based. The previous interaction history of the node is used to calculate its trust status, which is further used for access permission decision, as subsequently discussed.

In human terms, we only open our doors or give our keys to someone we trust not to be a criminal. Such trust may have built up through previous direct interactions or trusted recommendations. We employ this natural tool, without ignoring the fact that trust does not equal security ($Trust \neq Security$), but also acknowledging the close relationship between trust and security. In fact a study of current popular security approaches including public key cryptography reveals that they are not trust void. Most human-to-human, human-to-machine, and machine-to-machine interactions require trust to hold. Security systems can hardly stand a complete divorce with trust, since they cannot even be used if they are not trusted in any way. This close relationship between security and trust defines the motivation for the algorithm. The flowchart for the algorithm is presented in the next section.

3.1 Algorithm Flowchart

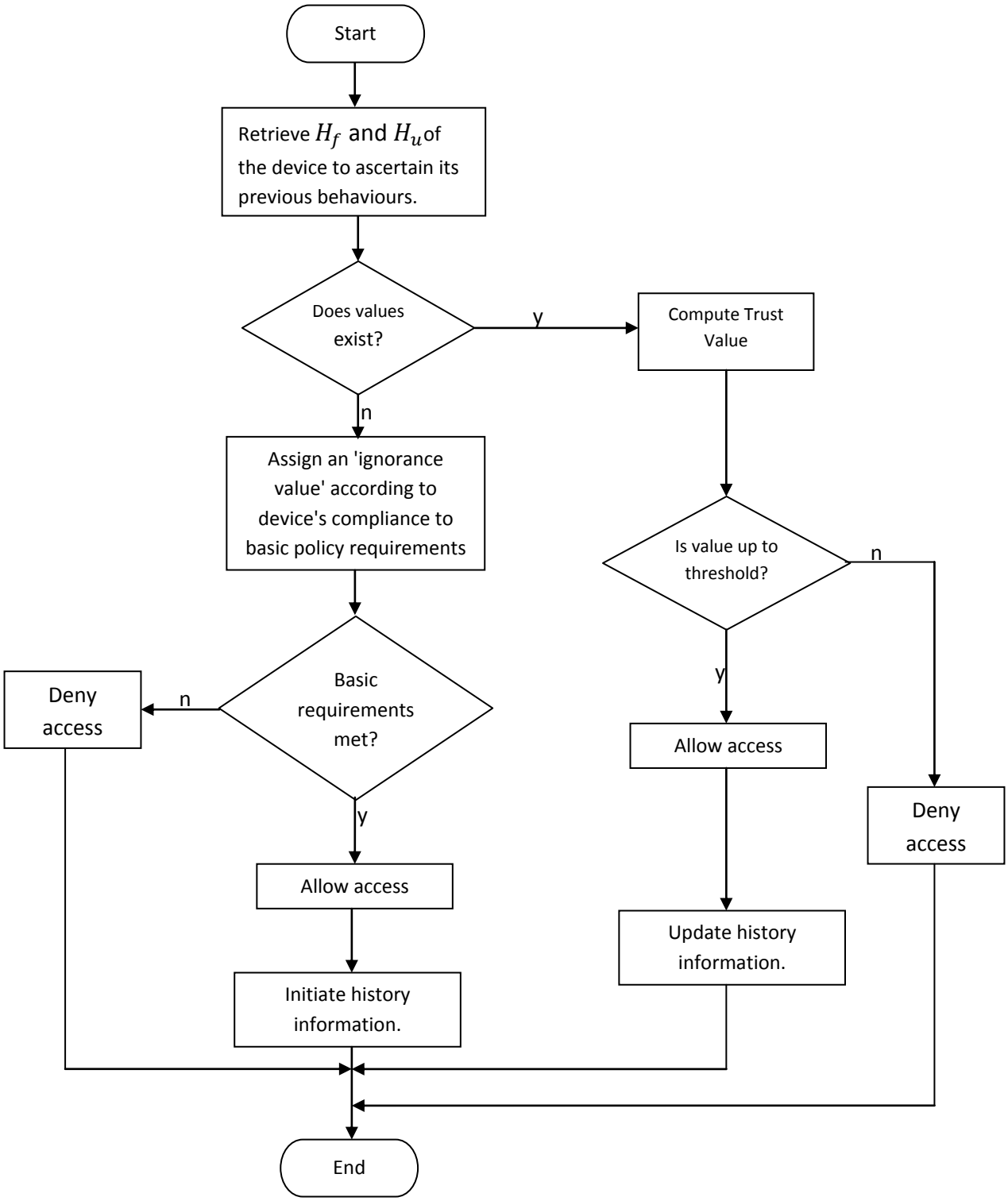


Figure 3.1: Algorithm Flowchart

H_f = number of previous favourable interactions

H_u = number of previous unfavourable (malicious) Interactions

y = yes

n = no

We refer to the whole process as trust engine. It starts by retrieving the interaction history of each node as it attempts accessing sensitive network resources. Using the information from the interaction history of the device which is already stored, the expected behaviour could be calculated based on probability. The number of favourable interactions is represented by H_f while that of the unfavourable (malicious) interaction is represented by H_u. We assume the existence of an intelligent system that keeps track of the behaviour of the nodes, and feeds the trust engine with necessary information. Such intelligent agent as also assumed in the risk model earlier discussed, will watch out for various forms of threat, especially the ones that lead to escalation of privilege; causing a node to access information which is not meant for it.

Information received from the intelligent system is used to update the interaction history of the nodes in the trust engine. Such information is kept to be used in calculating the expected behaviour when next the node attempts interacting with the network. If the probability suggests a trustworthy (or safe) behaviour, then access will be granted, else it will be denied. After each interaction with a device, the interaction history is usually updated to reflect its most recent behaviour. If the intelligent system reports a malicious act, the number of unfavourable (malicious) interaction (H_u) for such device will be increased by one, and the device will be dropped from the network for security reason. If there is no such alert, then it will be assumed that the device have behaved favourably, and then, the number of favourable interaction (H_f) will be increased by one at the end of the interaction. The steps involved in retrieving the favourable and malicious (unfavourable) interaction histories are as outlined below.

1: "Retrieve favourable interaction history"

2: for all $H_f \in$ (the behaviour history of nodes)

3: if H_f is for the current node, then

4: number of favourable interactions = H_f

5: else

6: keep on checking until the list is exhausted

7: end if

8: end for

9: end.

1: "Retrieve unfavourable interaction history"

2: for all $H_u \in$ (the behaviour history of nodes)

3: if H_u is for the current node, then

4: number of unfavourable interactions = H_u

5: else

6; keep checking until the list is exhausted

7: end if

8: end for

9: end

With the above steps, the number of favourable and unfavourable interactions will be retrieved and assigned to variables H_f and H_u respectively; which is subsequently used for the computation of the trust value as we shall see shortly. The next process after an exhaustive search of the interaction history is to determine if the device in question has any corresponding history information. To that end, If the list is exhausted without any matching value for H_f and/or H_u, then zero (0) will be assigned to each of them, to indicate that the device has no previous interaction with the network. The steps involved and the pseudo code are outlined below;

1: "does value exist?"

2: for all H_f and H_u belonging to the interaction history

3: if EOF then

4: if none of the history corresponds to the current device, then

5: H_f = 0

6: H_u = 0

7: end if

8: end if

9: end for

10: end

If this function holds (that is H_f = 0, and $H_u = 0$), it means that the device is joining the network for the first time, in which case, an ignorance value will be assigned as its first trust value; subject to meeting up the organisational specifications. Such specifications include; registration of the device, compliance with the device type specification, and the mode of connection to the network. If these conditions are met adequately, then a trust value which equals the trust threshold will be assigned to the node, if not, the first trust value will be assigned as zero (0); meaning a denial of access. The following steps explain the decision process for devices that are joining the network for the first time.

1: "First time devices"

2: if device is policy complaint then

3: $T_v = T_{min}$

4: else

5: T_v = 0

4: end if

5: end

The variable T_v refers to trust value, while T_{min} is the trust threshold. Depending on the assigned value, an access decision will be made, as follows;

1: "Allow or disallow access"

2: if $T_v \geq T_{min}$, then

3: Allow access

4: else

5: deny

6: end if

7: end

Once access is granted to a node, the trust engine listens to the intelligent system as discussed earlier for information on the behaviour of the node. If any malicious act is detected, and depending on the intensity, the device may be dropped to avoid further harm. After which the trust history of such randomly associated node is accordingly updated to reflect its most recent behaviour. This is usually done by updating the number of favourable and malicious interactions respectively. During the next access attempt by such node, the Trust value will be recalculated using the updated interaction history. The value of the probability based calculation suggests the next behaviour of the node.

However, recall that we have so far considered one of the possibilities; the other possibility is for devices that are not accessing the network for the first time, but already have interaction history with the trust engine. In this case to calculate the trust value (T_v), equation (3) above will be used, as shown in the following steps;

1: "Compute trust value for returning devices"

2: call "retrieve favourable interaction history"

3: call "retrieve unfavourable interaction history"

4: $T_v = E(p) = (H_f + 1)/(H_f + H_u + 2)$

5: call "allow or disallow access"

6: end.

Based on the outcome of the computation, an access decision will be made; leading to allowing or disallowing access as outlined earlier in the "allow or disallow access" steps. If a node is denied access, no further action is required of the system concerning its interaction history, but if the node is allowed access, it is being monitored by the intelligent system during its whole interaction, and after such interaction(s), the history will be updated accordingly.

3.2 Pseudo Code

The pseudo code for the algorithm is thus summarised;

START

GET H_f and H_u
numOfFaint = H_f
numOfUnint = H_u

IF ((numOfFaint == 0) & (numOfUnint == 0))

IF (Device meet company policy)

$T_v = T_{min}$

Allow Access

Initiate History Information

ELSE

Deny Access

ELSE

IF ((ComputeTrust(numOfFaint, numOfUnint)) < T_{min})

Deny Access

ELSE

Allow Access

Update History Information

END IF

ComputeTrust(H_f, H_u) //Function to compute trust

trust = $T_v = E(p) = (H_f + 1)/(H_f + H_u + 2)$

RETURN (trust)

END

3.3 Mathematical Representation

Most trust model present recommendations as a way of building initial trust for first time users. This is a good way of obtaining trust especially in a kind of e-commerce and similar environments where users have never had any form of prior contact. A close view at BYOD however suggests that most attention is usually on the employees; bringing their own devices to work and using them for official functions. For someone to be an employee in any organisation, it implies that there has been a kind of prior contact, not necessarily with the network, but obviously with the organisation. Such employee is also bound to observe the policies of the organisation. Accordingly, researchers have recommended appropriate policy enforcement as the way forward for BYOD based organisations. Among such policies include: registration of the employees' mobile devices, recommendations on mobile devices the organisation would tolerate, and operating system versions allowed. Context such as the

type of network through which the device is connecting have also been identified as crucial in making security decisions regarding mobile devices. (Armando, Costa & Merlo, 2013) (Park, Han & Chung, 2006) (Singh, 2012) (Mansfield-Devine, 2012).

3.2.1 First Time Devices

Access decision for first time devices are based on policy compliance such as the ones outlined earlier, after which the interaction history will be maintained and used for subsequent access decisions. An ignorance value expressed as $R \in \{0, T_{min}\}$ is assigned to a first time device which has no previous interaction history with the network. The value to be assigned will be based on compliance with the organisational policies on; device registration, approved device type, and operating system version.

$$T_v = \begin{cases} T_{min} \\ \\ 0 \end{cases} \quad 0 \leq T_v \leq T_{min}$$

If for instance a new employee arrives an organisation and have not used the organisation network resources previously; then, adequately fulfilling these conditions will determine if access will be granted or denied. If the device meets up with the security requirements which shall be automatically checked on attempt to access network resources, then an initial trust value that is equal to the minimum threshold ($T_v = T_{min}$) will be assigned to allow it access to the network for the first time. However if the policies are not adequately met, a value less than the threshold ($T_v < T_{min}$) will be assigned to it; usually 0, thus disqualifying it access to the network.

3.2.2 Returning Devices

This refers to devices which are not accessing the network for the first time, but already has previous interactions history. In this case, beta distribution concept is used to determine the

probability of its next behaviour, to predict safe or unsafe devices beforehand. An interaction history is usually maintained by frequent update of the number of previous favourable and unfavourable interactions. We denote the number of favourable interactions of a given device with H_f, and that of unfavourable interactions with H_u. We define unfavourable interaction as that in which the assumed intelligent system as discussed earlier reports a malicious activity concerning the device; in such case, $H_u = H_u + +$. If on the contrary, a device interacts with the network without being reported until its interaction at that moment is over, then it is termed favourable; therefore the number of favourable interaction is updated just before it leaves the network; $H_f = H_f + +$.

Recall the beta distribution equation (1) in the previous chapter (Ping&Jing, 2007) (Sun&Denko, 2008);

$$f(p|\alpha,\beta) = \frac{\gamma(\alpha + \beta)}{\gamma(\alpha)\gamma(\beta)} p^{\alpha-1}(1-p)^{\beta-1}$$

Where $0 \leq p \leq 1$, $\alpha > 0$, and $\beta > 0$.

Recall also the expression for calculating the expected of beta distribution value as in equation (2);

$$E(p) = \frac{\alpha}{\alpha + \beta}$$

We associate the number of favourable interactions to α, and the number of unfavourable interactions to β;

$$\alpha = H_f + 1,$$

and

$$\beta = H_u + 1$$

Thus equation (2) can be expressed;

$$T_v = E(p) = \frac{H_f + 1}{H_f + H_u + 2} \quad 3$$

Where H_f = the number of favourable interaction for a given device,

H_u = the number of unfavourable interaction of same device, and

T_v = the trust value of the devices

$E(p)$ = expected probability of nodes' behaviour (favourable or unfavourable (malicious)).

Notice that T_v is expected, meaning that it is being calculated from the already gathered information as a probability.

After the above calculation is made, and a trust value (T_v) for the associating node determined, a comparison of the trust value (T_v) and the trust threshold (T_{min}) will be made. Access will be allowed if the calculated trust value is greater or equal to the trust threshold ($T_v \geq T_{min}$).

3.3 Result and Analysis

In this section, we shall discuss the expected result of our algorithm, based on the earlier explained mathematical expressions and assumption. When a device attempts access and did not comply with the basic security policies, it will be dropped and no further action will be required of the system. But if the node is granted a pass after fulfilling the set criteria, then it will be further monitored, and its behavioural history adequately updated; to be used for subsequent access permission decision.

3.3.1 Effect of favourable (secure) interactions (H_f)

Tables 3.1 below represent the interaction history of device A, with increasing number favourable interactions (H_f). Equation (3) is used to calculate the trust value (T_v). Increase in trust value as the number of interaction increases, demonstrates that trust grows with increase in favourable (secure) interactions. Although trust in not equal to security, detecting and stopping malicious nodes beforehand potentially implies enhanced security for the network; the less threat a network is vulnerable to, the more secure it could be. In our scenario, increase in trust value suggests a less possibility of a device posing security threat to the network. This in-turn suggests a higher possibility of subsequent secure interaction; thus encouraging more secure BYOD network. Increase in the number of secure interactions of a node (favourable interaction (H_f)) leads to increased trust on that node, as the table suggests, and an increase in trust suggests an increased certainty of secure behaviour of the node if allowed access to the network. If a device is separated from the network for lack of safe reputation for instance, it significantly reduces the system's exposure to potential threats, implying more security.

The graphical representation of this is given in figure 3.1. It is noteworthy to observe that the proportional increase of the H_f and T_v became more significant as the number of interactions increased more; implying that if a node has for a long period of time acted safe, the probability of its continual safe acts is considerably high, and making a security decision with the consideration that it is going to act safe will most likely yield a favourable result.

Table 3.1: Interaction History for Device "A" with Increasing Favourable Behaviour.

Number of previous interaction	Number of previous unfavourable interactions (H_u)	Number of previous favourable interactions (H_f)	Calculated trust value (T_v)	Access Decision
2	1	1	0.5	Pass
10	1	9	0.833	Pass

20	1	19	0.909	Pass
30	1	29	0.937	Pass
40	1	39	0.952	Pass
50	1	49	0.961	Pass
60	1	59	0.967	Pass
70	1	69	0.972	Pass
80	1	79	0.975	Pass
90	1	89	0.978	Pass
100	1	99	0.980	Pass

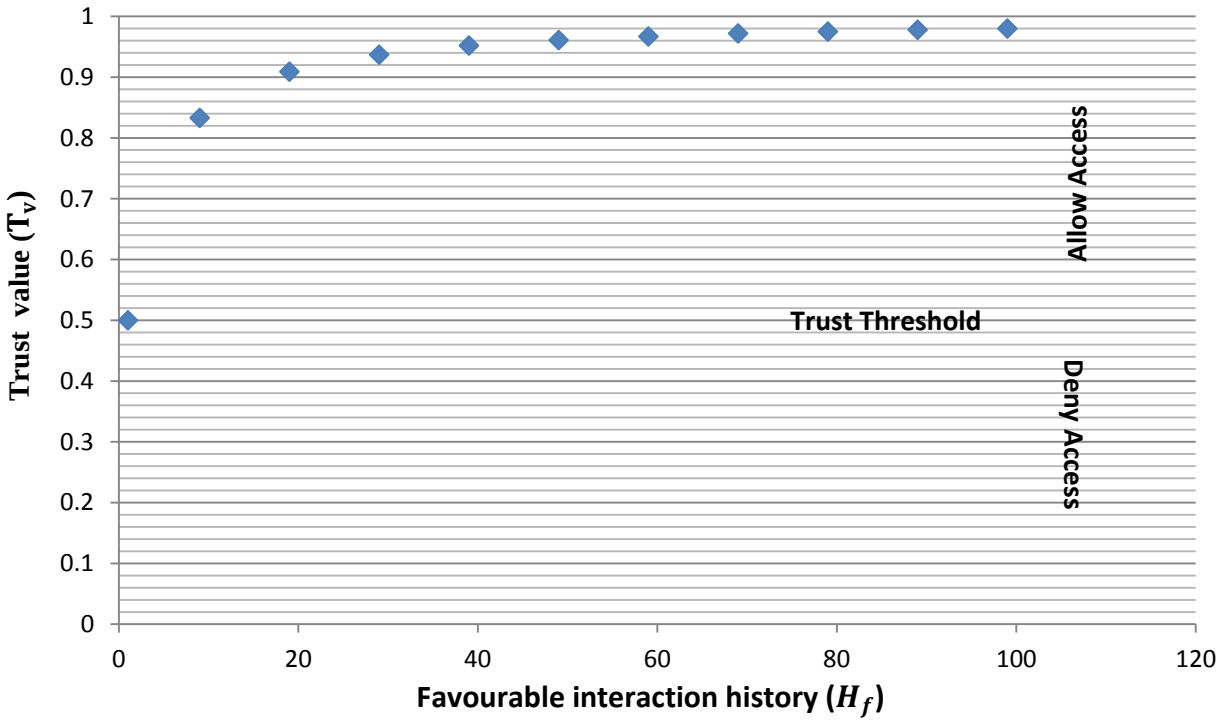


Figure 3.2: Effect of Favourable (secure) Interactions (H_f) on Trust Value (T_v) and Access Decision

3.3.2 Effect of Unfavourable (malicious) interactions

Table 3.2 shows a drop in trust due to past malicious interaction history of the nodes. This consequently resulted to denial of access to the network, to keep such nodes from threatening

the entire network. A drop in trust here indicates that trust can be destroyed by malicious interactions just as the security of any system can be jeopardized by malicious activities. Indeed, trust can be destroyed even quicker than it took to build it. The same equation (3) is used for calculating the trust value (T_v) in the table.

Table 3.2: Interaction History for Device "B" with increasing unfavourable (malicious) behaviour.

Number of previous interaction	Number of previous unfavourable interactions (H_u)	Number of previous favourable interactions (H_f)	Calculated trust value (T_v)	Access Decision
2	1	1	0.5	Pass
10	9	1	0.1666	Deny
20	19	1	0.0909	Deny
30	29	1	0.0652	Deny
40	39	1	0.0476	Deny
50	49	1	0.0384	Deny
60	59	1	0.0322	Deny
70	69	1	0.0277	Deny
80	79	1	0.0243	Deny
90	89	1	0.0217	Deny
100	99	1	0.0196	Deny

The graphical representation of this table is presented in figure 3.2 below;

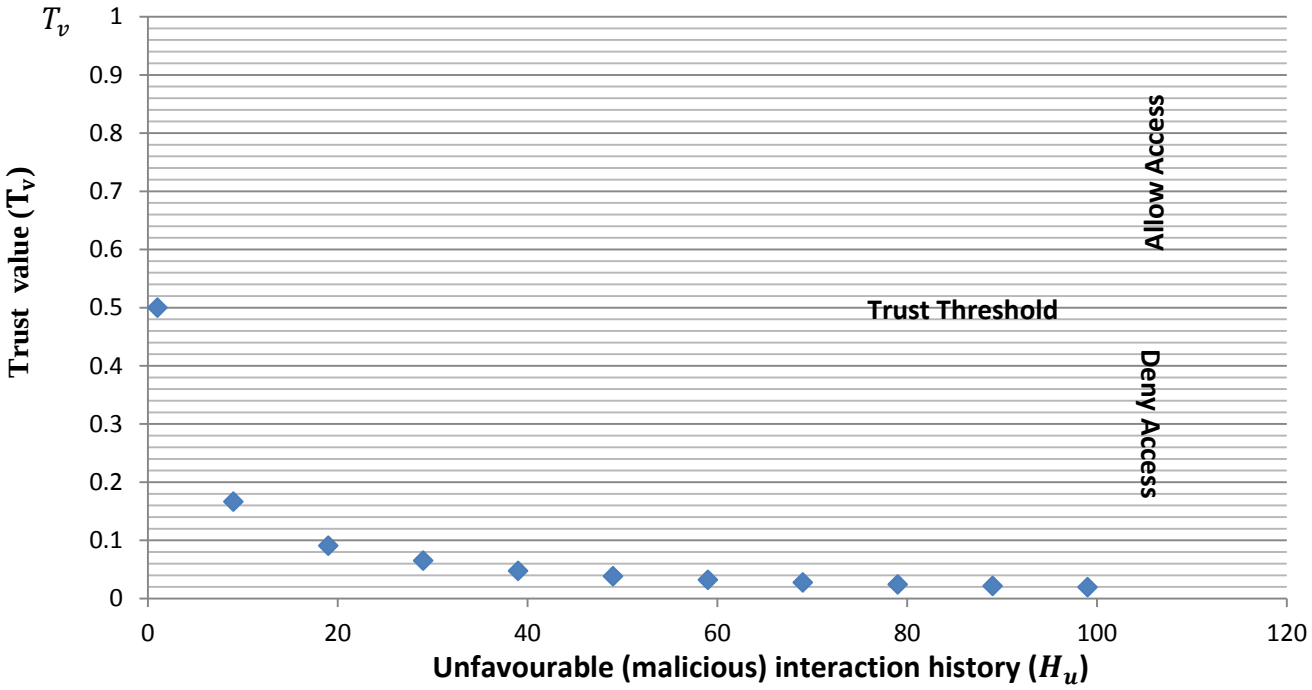


Figure 3.3: Effect of Unfavourable (malicious) Interactions (H_u) on Trust Value (T_v) and Access Decision

Figures 3.1 and 3.2 can be reproduced into one as shown in figure 3.3 below to contain both the favourable and unfavourable interactions;

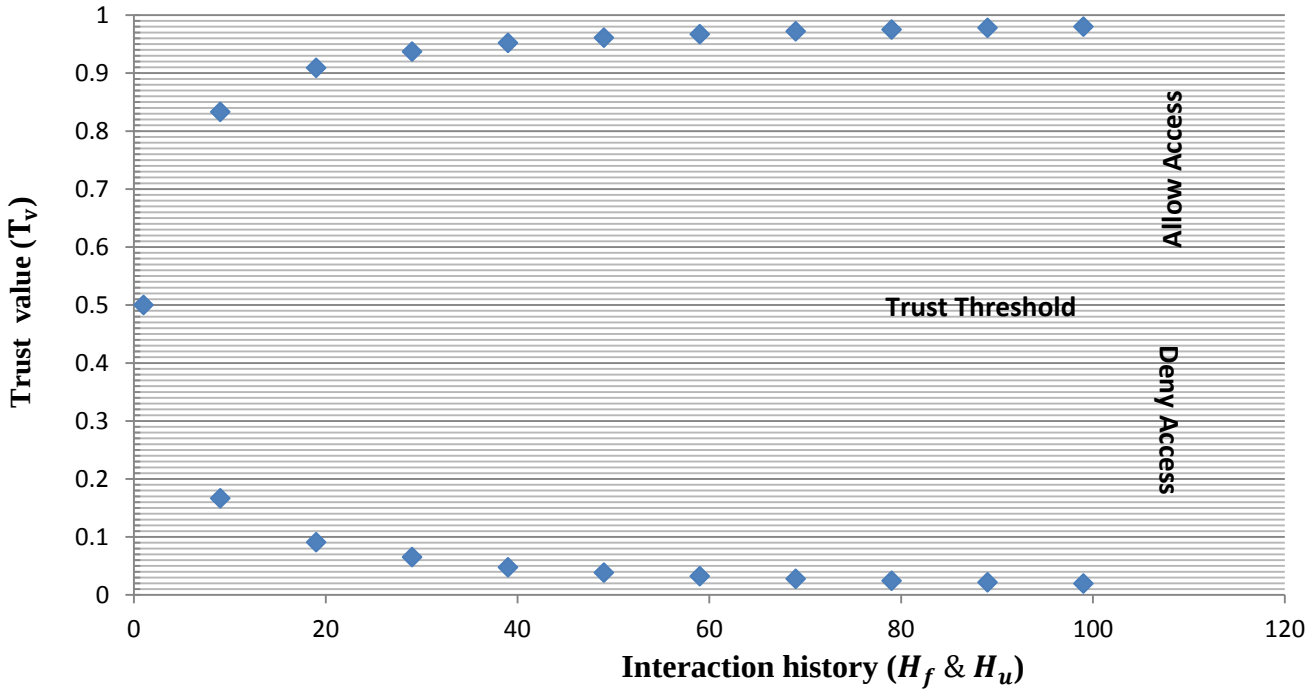


Figure 3.4: Effects of Favourable (H_f) and Unfavourable (H_u) Interactions on Trust Value (T_v) and Access Decision.

As introduced earlier in the chapter, we relate trust values to the device's possibility of acting safe if allowed access to the network. The increase and decrease in trust values as illustrated with the above tables and figures, also represent an increase and decrease in the possibility of devices acting safe or unsafe when access is granted to the network. If devices with malicious intents are screened out of the network, then the security is surely increased, thus the aim of a more dynamic access control approach that can enhance the security of BYOD network.

3.4 Comparison with the Existing System

Trust and reputation approaches have been proposed and applied in a many dynamic environments as discussed in previous chapter, but has not been specifically channelled towards tackling the dynamic security needs of BYOD network, probably because the concept is relatively new. The recently published approach in (Armando, Gabriele & Merlo, 2013), suggests the most recent face of BYOD security approach. As reviewed earlier, their proposed security framework forbids a device from installing applications that do not conform to the policy of the organisation. This seems to take care of only threats originating from applications that have been considered unsafe. Though a good move, we consider this not dynamic enough following the roaming nature of mobile devices in and out of compliance. Even a device that did not download any incriminating application, can be corrupted by others, through mutual collaboration; thereby posing threat to the network. There is therefore a need for a more dynamic system to monitor the interactions of nodes; sieving malicious nodes out of the network and allowing the safe ones to interact.

The proposed algorithm not only discourages users (employees) from installing malicious applications to enable them maintain access to the network, but watches out for other forms of malicious activities of any connected node, acknowledging that mobile devices roam in and out of compliance easily. Malicious nodes are dropped out of the network, and a history record kept against it, for subsequent access permission decision. Using the interaction history of devices "A" and "B" earlier computed in tables 3.1 and 3.2, we illustrate with the following graph, how our approach disallowed the malicious device and allowed the non-

malicious device; based on trust values calculated from their past interaction experiences. But the security framework of (Armando, Gabriele & Merlo, 2013) responded indifferently; granting access to the devices based on a constant threshold of policy compliance; which is only considered as minimum initial threshold in the proposed algorithm.

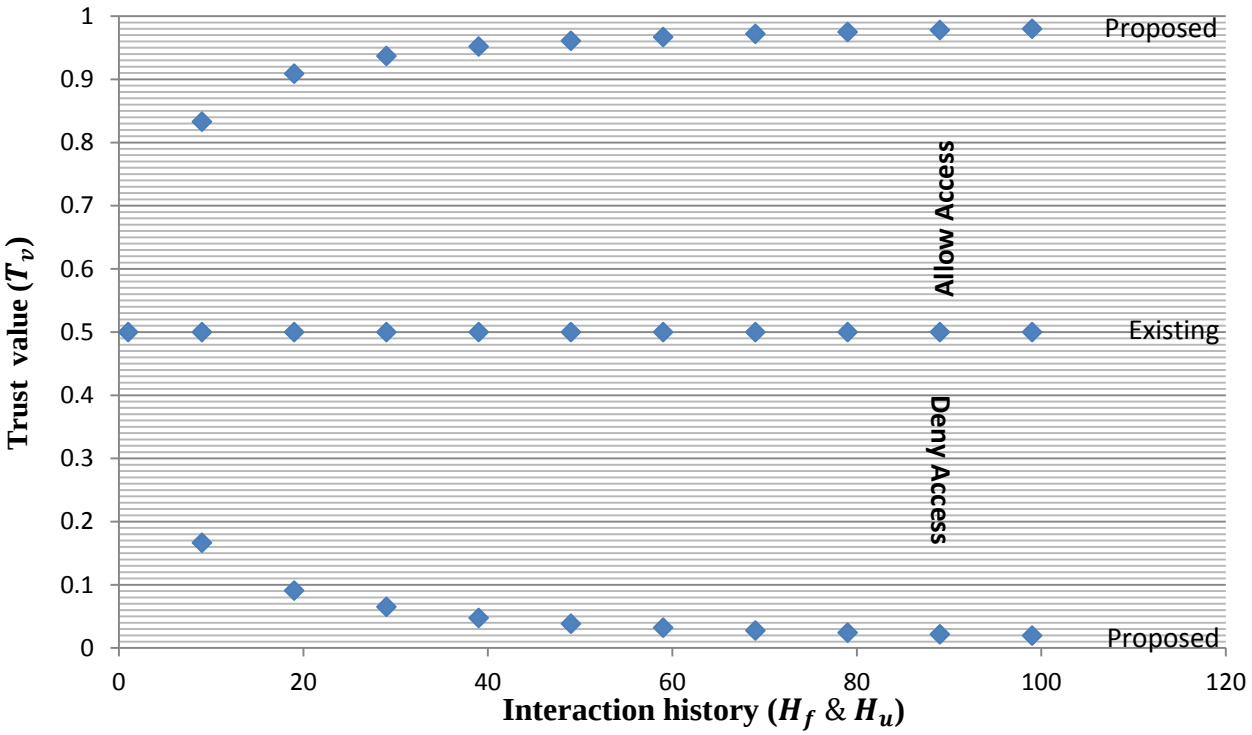


Figure 3.5: A comparison with the existing system.

It could be seen from figure 3.3 that the existing system tends to be careless about what goes on with the nodes after the initial security policy is met. Efforts are only made to enforce the policy of not installing malicious applications on devices, however the dynamism of the devices is not adequately considered. For instance, provided a device did not directly install any prohibited application, it will continue to access the network even if it gets contaminated through other numerous means such as infection from collaborating with other devices; and thus continue to terrorise the network unchecked. The proposed algorithm goes beyond just the initial stage of ensuring that device complies with the security policies (trust threshold) to further check their subsequent behaviour, in order to detect when they start acting malicious.

Such past behaviour history is also used to detect potentially malicious nodes and stop them beforehand from compromising the entire network.

Only devices with clear possibility of acting safely are allowed to access the network. Those with malicious intent are dropped as a way of keeping the network safe from potential threats. With the proposed approach, employees will be left with no choice than to avoid all possible malicious encounters, update their devices with necessary security applications, and avoid malicious applications that could cause them access denial. Through this means, the over-all potential security of the network is enhanced.

3.5 Summary

In this chapter, we have presented the proposed algorithm, starting with flowchart representation and a breakdown of each of the flowchart block, as well as the pseudo code for the algorithm. A mathematical expression for calculating the expected trust value of each randomly associated node have also been presented, and the appropriate explanations given for both first-time and returning devices. A sample computation with the presented mathematical expression have also been given to illustrate how effective the algorithm can be in real time network, and finally, a comparison with the existing system was made with a justification of an improved security compliance.

CHAPTER FIVE

CONCLUSION AND FUTURE WORK

5.1 Conclusion

This study has shown that BYOD is a relatively new concept with an alarming popularity among corporate organisations and enterprises. The concept have been predicted to see even a more rapid growth in the near future. As organisations migrate from their usual traditional network setting towards it, they also inherit its security challenges, which if not adequately handled, can cancel the anticipated advantages. The dominance of mobile devices in BYOD environments speak much about its security limitations, minding the fact that mobile devices themselves have more limitations even in resources compared to stationary or relatively stationary computers.

The review of literature in the chapter two has revealed trust as a viable means of dynamically ascertaining beforehand if an agent is fit to be engaged with in a transaction. It has been applied in many pervasive environments such as e-commerce with commendable results. The success story of trust made it our choice of approach to engage in addressing the security needs of BYOD network.

Similarly, access control has been identified as a focal point when considering the security of any system; whether digital or physical. Therefore to adequately address the security need of BYOD, there is need to sieve what enters the network in a dynamic manner; keeping the nodes with malicious intent out of the network, to stop them from threatening the entire network. To this end, the proposed algorithm as presented in chapter three employs the concept of trust to check the randomly associated nodes at their entry points; predicting those with malicious intents and denying them access, as a way of saving the network from potential threats.

The flowchart of the proposed algorithm and the explanation of its steps are presented in chapter three, alongside the involved mathematical processes through which a node is tagged potentially malicious (unfavourable) or safe (favourable). Previous interaction histories of the randomly associated nodes are the basic inputs into the mathematical equation. They are used to calculate the level of trust of the nodes as a representation of their potential behaviour. A sample calculation is also made to demonstrate how the system could dictate potentially malicious nodes from the safe ones.

Compared to the existing model in BYOD which only prohibits the installation of malicious applications in the mobile devices without any means of checking its actual behaviour on the network, the proposed approach proved more security compliant by providing for; (i) placing a check on the devices as they access and interact with the network, (ii) keeping record of their interaction history and using it to predict the would be behaviour of the device when next they interact, and (iii) blocking potentially malicious nodes from compromising the entire network.

This work has therefore adequately explored the concepts of BYOD, its advantages and security limitations. Trust has also been thoroughly discussed, including its related applications. We have also done justice to various access control models, highlighting their strengths and weaknesses as bases for our approach. Finally, the proposed algorithm have employed the concept of trust on the access control system of BYOD in a manner that allow for adequate dynamism and enhanced security of the network.

5.2 Future Work

As pointed out earlier, the proposed algorithm has some limitations which could be built upon in the future. The assumed intelligent system could be a good area for future work; a BYOD based system that can sense the organisational policy requirements on devices as they request access permission, and monitor the entire interaction to update the trust engine accordingly. Similarly the model can be improved by carefully making provision for recommendations, and the effect of time on the interaction history, in a BYOD compatible manner.

REFERENCES

Armando, A., Kessler, F.B., Costa, G., Merlo, A. & Verderame, L. (2009) 'Bring your own device securely', *Proceedings of the 28th Annual ACM Symposium on Applied Computing* (SAC '13), pp.1852-1858**.**

Bijon, K.Z., Krishnan, R. & Sandhu, R. (2012) *'Risk-aware RBAC sessions',* in Anonymous *Information systems security.* Springer. pp. 59-74.

Chin, S. & Older, S. (2010) *Access control, security, and trust: A logical approach.* CRC press.

Cutillo, L.A., Molva, R. & Strufe, T. (2009) 'Safebook: A privacy-preserving online social network leveraging on real-life trust', *Communications Magazine, IEEE,* 47 (12), pp.94-101.

Deno, M.K. & Sun, T. (2008) "Probabilistic trust management in pervasive computing", *Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on,* IEEE. p610-615.

Ferraiolo, D.F. & Kuhn, D.R. (2009) 'Role-based access controls', *ArXiv Preprint arXiv:0903.2171,* .

Furtmüller, F.G. (2013) 'An approach to secure mobile enterprise architectures', .

Gambetta, D. (2000a) 'Can we trust trust', *Trust: Making and Breaking Cooperative Relations,* 2000 pp.213-237.

Ghosh, A., Gajar, P.K. & Rai, S. (2013) 'Bring your own device (BYOD): security risks and mitigating strategies', *Journal of Global Research in Computer Science,* 4 (4), pp.62-70.

Giorgini, P., Mouratidis, H. & Zannone, N. (2006) 'Modelling security and trust with secure tropos', *Integrating Security and Software Engineering: Advances and Future Vision,* pp.160-189.

Hong, X., Huang, D., Gerla, M. & Cao, Z. (2008) "Sat: Building new trust architecture for vehicular networks", *Proceedings of the 3rd ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch),* .

Hsu, M., Ju, T.L., Yen, C. & Chang, C. (2007) 'Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations', *International Journal of Human-Computer Studies,* 65 (2), pp.153-169.

Jin, X., Krishnan, R. & Sandhu, R. (2012) *'A unified attribute-based access control model covering dac, mac and rbac',* in Anonymous *Data and applications security and privacy XXVI.* Springer. pp. 41-55.

Jøsang, A. (2001) 'A logic for uncertain probabilities', *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems,* 9 (03), pp.279-311.

Jøsang, A., Ismail, R. & Boyd, C. (2007) 'A survey of trust and reputation systems for online service provision', *Decision Support Systems,* 43 (2), pp.618-644.

Lagesse, B., Kumar, M., Paluska, J.M. & Wright, M. (2009) "Dtt: A distributed trust toolkit for pervasive systems", *Pervasive Computing and Communications, 2009. PerCom 2009. IEEE International Conference on,* IEEE. p1-8.

Lamsal, P. (2001) 'Understanding trust and security', *Department of Computer Science, University of Helsinki, Finland,* .

Lang, B., Foster, I., Siebenlist, F., Ananthakrishnan, R. & Freeman, T. (2009) 'A flexible attribute based access control method for grid computing', *Journal of Grid Computing,* 7 (2), pp.169-180.

Lee, J., Kim, H. & Hong, J.S. (2008) "An attribute aggregation architecture with trust-based evaluation for access control", *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE,* IEEE. p1011-1014.

Mansfield-Devine, S. (2012) 'Interview: BYOD and the enterprise network', *Computer Fraud & Security,* 2012 (4), pp.14-17.

Mármol, F.G. & Pérez, G.M. (2009) "TRMSim-WSN, trust and reputation models simulator for wireless sensor networks", *Communications, 2009. ICC'09. IEEE International Conference on,* IEEE. p1-5.

Mohammed, L. (2008) "Towards pervasive computing security", *The Proceedings of the World Congress on Engineering,* Citeseer.

MobileIron (2011) *Building Bring-Your-Own-Device" (BYOD) Strategies,* Viewed 20 March 2013, http://www.webtorials.com/main/resource/papers/mobileiron/paper1/byod_part_1.pdf>

Park, S., Han, Y. & Chung, T. (2006) *'Context-role based access control for context-aware application',* in Anonymous *High performance computing and communications.* Springer. pp. 572-580.

Parno, B., McCune, J.M. & Perrig, A. (2010) "Bootstrapping trust in commodity computers", *Security and Privacy (SP), 2010 IEEE Symposium on,* IEEE. p414-429.

Ping, W. & Jing, Q. (2007) "A mathematical trust model in e-commerce", *Multimedia and Ubiquitous Engineering, 2007. MUE'07. International Conference on,* IEEE. p644-649.

Scarfo, A. (2012) "New security perspectives around BYOD", *Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on,* IEEE. p446-451.

Shuai, Z., Fen, X., Yang, X., Yi-xian, Y. & Zheng-ming, H. (2010) "Trust model based on dynamic policy similarity for pervasive computing environments", *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, IEEE. pV4-476-V4-479.

Singh, M.N. (2012) 'BYOD genie is out of the Bottle–"Devil or angel"', *Journal of Business Management & Social Sciences Research (JBM&SSR) 2012*.

Sun, T. & Denko, M.K. (2008) "Performance evaluation of trust management in pervasive computing", *Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on*, IEEE. p386-394.

Wang, B., Wong, C.M., Wan, F., Mak, P.U., Mak, P.I. & Vai, M.I. (2010) "Gaussian mixture model based on genetic algorithm for brain-computer interface", *Image and Signal Processing (CISP), 2010 3rd International Congress on*, IEEE. p4079-4083.

Wang, Y. & Singh, M.P. (2007) "Formal trust model for multiagent systems", *Proceedings of the 20th International Joint Conference on Artificial Intelligence (IJCAI)*, p1551-1556.

Yuan, E. & Tong, J. (2005) "Attributed based access control (ABAC) for web services", *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on*, IEEE.

Zineddine, M. & Kindi, H. (2012)'Smart phones: Another IT security scuffle', *International Conference on Internet Computing , Informatics in E-Business and applied Computing (ICIEACS 2012)* .

APPENDIX A

MSC PROJECT PROPOSAL FORM

AY12/13, Semester 1

Student Number	1029282
Student Name	Francis N. Nwebonyi
Degree Course	MSc Computer Security and Forensics.
Supervisor Name	Dr. Gregory Epiphaniou
Title of Project	An Access Control System to Improve Security Amongst Randomly Associated Nodes in BYOD Network.
Description of your artefact	Bring Your Own Device (BYOD) is a concept that allow employees to bring personally owned (mobile) devices for official work. It comes with many benefits such as reduced cost and enhanced efficiency, but also with some security concerns which must be addressed to unveil its full potentials. (Bernhard et al.,)(Miller, Voas & Hurlburt, 2012). A close look at the traditional access control models (such as Role Based Access Control, Mandatory Access Control and Discretionary Access Control) reveal that attention is always focused on individual users, and nothing about devices being used. This approach may have been working in traditional network settings because the organisations take full ownership of the devices and to a reasonable extent ensures its security. However, in BYOD where the possession of devices is lost to the employees (users), it is very important to automatically check any device for policy compliance before they are allowed access to the network and its recourses. The fact that mobile devices easily forms collaborative network makes them very much more prone to malware and virus attacks, as well as other forms of compromise, than stationary devices. Therefore allowing such (mobile) devices to access the network without checks, simply equals to no security at all. (Toninelli et al., 2006)(Mansfield-Devine, 2012)(Ferraiolo&Kuhn, 2009).

Accordingly, there is need for an access control system dedicated to BYOD networks, such that adequate security policies will be accommodated as part of the constraints that must be fulfilled before access to the network is granted. We propose an algorithm for device aware access control mechanism based on trust concepts, in which the previous behaviour of randomly associated nodes are used to infer how securely they will behave in the future.

Aim and Objectives

The aim of this work is to derive an algorithm for a device aware access control system that increases the security BYOD networks based on trust. The algorithm is to ascertain the trust worthiness of interacting nodes beforehand via trust value computation, which is then used for access permission decision. This is geared towards securing the network resources by dictating and dropping malicious (non trustworthy) node(s) out of the network to prevent it from causing security breaches. The past behaviour of devices will be used to infer the next behaviour when it connects to the network, in order to determine if it merits a pass to the network resources or otherwise.

The following objectives shall be achieved;

- Extensive review of existing access control and trust models.
- Deriving suitable parameters for acquiring and monitoring interaction history of the randomly associated nodes.
- Deriving a mathematical method of computing trust value of nodes, which also portray their expected behaviour if allowed access to the network.

	• Proposing a trust based algorithm for screening out malicious nodes in a BYOD network, as a way of increasing its security. The past interactions of each randomly associated node will be used to calculate its subsequent security behaviour using the principles of probability theory. <u>List of features that the artefact will include:</u> • A highlight on probability theorem upon which our algorithm will be based. • Mathlab tool. • Necessary codecs of a chosen Programming Language.
What methodology (structured process) will you be following to realise your artefact?	The algorithm will be based on probability theory and the steps shall be explained using flowcharts, while Mathlab will be used to implement the codes. The artefact shall be accomplished using Waterfall model; owing to the simplicity of its usage, and its provision for stage by stage completion of task blocks.
How does your project relate to your degree course and build upon the units/knowledge you have studied/acquired	This project is strongly security based and directly relates to my course of study; MSc Computer Security and Forensics. The units I have studied as listed below, have laid the foundation I would need to accomplish this task; Network Administration and Management, Advanced Security and Counter Measures, Cryptography, Professional Project Management, Computer Security, Network Systems, Advanced Digital Forensics, and Forensic Data Acquisition and Analysis
Resources	The following resources will be needed for the development of the artefact and the whole completion of the work; • Conference and Journal papers will be needed in their volumes to gain full grasp of the works already done in related fields. • A Computer System running Windows 7 Operating System. • Mathlab tool. • Chosen Programming Language.

Have you completed & submitted your ethics form?	Yes	

Bernhard, J., Bixler, R., Choudhury, O., McBurney, W. & Purta, R. 'BYOD VMs mini project', .

Ferraiolo, D.F. & Kuhn, D.R. (2009) 'Role-based access controls', *ArXiv Preprint arXiv:0903.2171*, .

Mansfield-Devine, S. (2012) 'Interview: BYOD and the enterprise network', *Computer Fraud & Security*, 2012 (4), pp.14-17.

Miller, K.W., Voas, J. & Hurlburt, G.F. (2012) 'BYOD: Security and privacy considerations', *IT Professional*, 14 (5), pp.53-55.

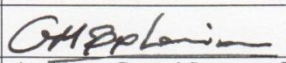
Toninelli, A., Montanari, R., Kagal, L. & Lassila, O. (2006) 'A semantic context-aware access control framework for secure collaborations in pervasive computing environments', *The Semantic Web-ISWC 2006*, pp.473-486.

APPENDIX B

ETHICS FORM

FACULTY OF CREATIVE ARTS, TECHNOLOGIES AND SCIENCE

Form for Research Ethics Projects (CATSethicsform)

1. Student Name	Francis N. Nwebonyi
2. Student Number:	1029282
3. Degree Pathway:	MSc Computer Security and Forensics
4. Supervisor's name	Gregory Epiphaniou
5. Supervisor Signature	
6. Working title of project	An Access Control System to Improve Security Amongst Randomly Associated Nodes in BYOD network.

SECTION A Proposal

Please summarise below the ethical issues involved in the research proposal and how they will be addressed. In any proposal involving human participants clear explanation of how informed consent will be obtained, how confidentiality will be observed, how the nature of the research and the means of dissemination of the outcomes will be communicated to participants must be provided.

This project investigates the unique security features of BYOD (Bring Your Own Device) networks, and critically reviews the existing Access Control systems, to identify their strengths and weaknesses with regard to BYOD. Based on the findings, a provable enhancement will be proposed to arrive at an Access Control system that is more suitable for BYOD.

It therefore do not have any ethical issues, all required experiments will be carried out in an isolated system to ensure accuracy and avoid distortion(s) that may arise from environmental factors.

SECTION B Check List

Please answer the following questions by circling **YES** or **NO** as appropriate.

1. Does the study involve vulnerable participants or those unable to give informed consent (e.g. children, people with learning disabilities, your own students)?

   YES (**NO**)

2. Will the study require permission of a gatekeeper for access to participants (e.g. schools, self-help groups, residential homes)?

   YES (**NO**)

3. Will it be necessary for participants to be involved without consent (e.g. covert observation in non-public places)?

   YES (**NO**)

4. Will the study involve sensitive topics (e.g. obtaining information about sexual activity, substance abuse)?

   YES (**NO**)

5. Will blood, tissue samples or any other substances be taken from participants?

   YES (**NO**)

6. Will the research involve intrusive interventions (e.g. the administration of drugs, hypnosis, physical exercise)?

   YES (**NO**)

7. Will financial or other inducements be offered to participants (except reasonable expenses or small tokens of appreciation)?

   YES (**NO**)

8. Will the research investigate any aspect of illegal activity (e.g. drugs, crime, underage alcohol consumption or sexual activity)?

   YES (**NO**)

9. Will participants be stressed beyond what is considered normal for them?

   YES (**NO**)

10. Will the study involve participants from the NHS (patients or staff) or will data be obtained from NHS premises?

    YES (**NO**)

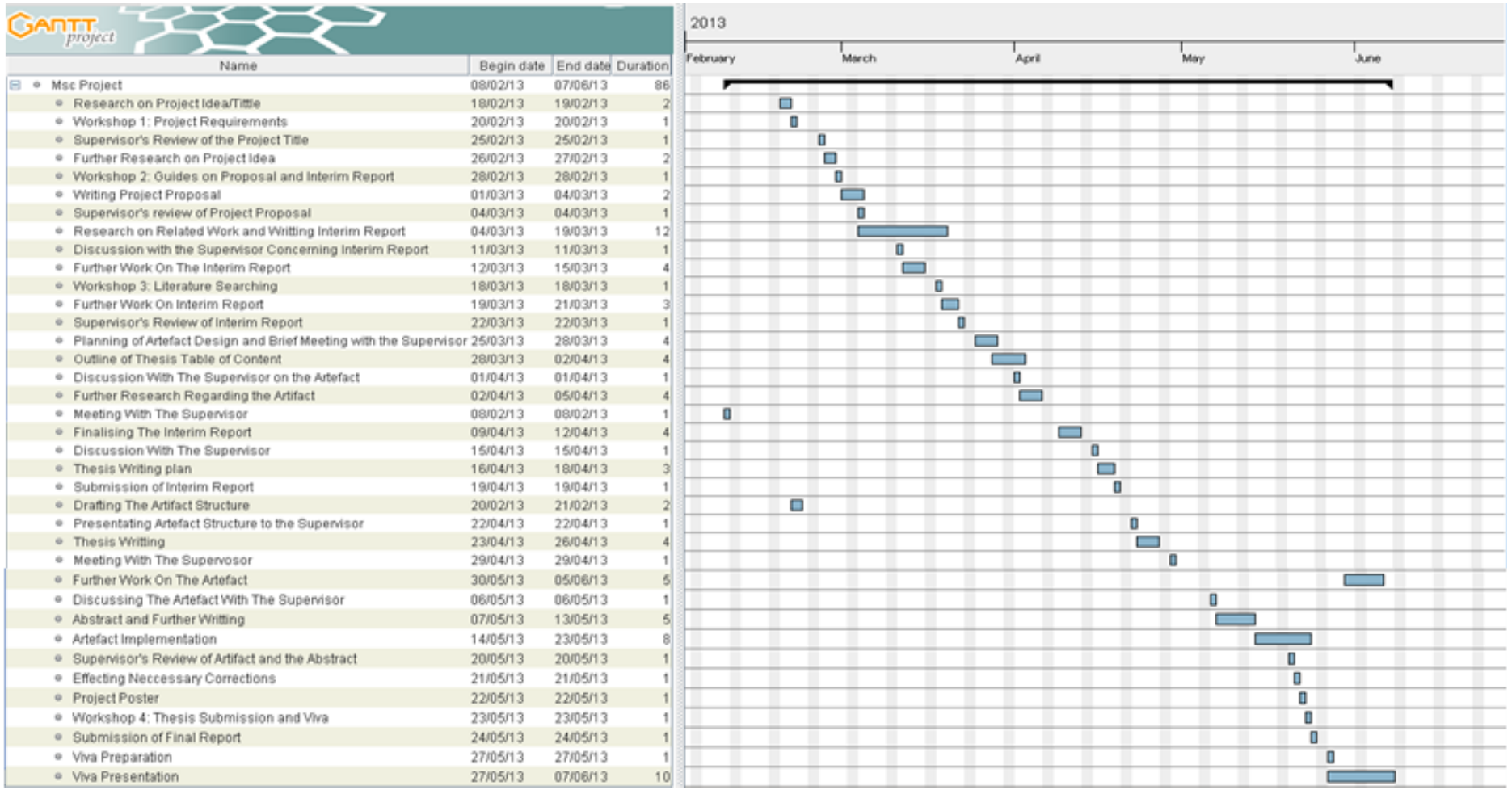
If the answer to any of the questions above is "Yes", or if there are any other significant ethical issues, then further ethical consideration is required. Please document carefully how these issues will be addressed.

Signed (student): NKO Date: 07-03-2013.

Countersigned (Supervisor): Date: 07/03/2013

APPENDIX C

GANTT CHART SHOWING PROJECT PLAN



Name	Begin date	End date	Duration
Msc Project	08/02/13	07/06/13	86
Research on Project Idea/Tittle	18/02/13	19/02/13	2
Workshop 1: Project Requirements	20/02/13	20/02/13	1
Supervisor's Review of the Project Title	25/02/13	25/02/13	1
Further Research on Project Idea	26/02/13	27/02/13	2
Workshop 2: Guides on Proposal and Interim Report	28/02/13	28/02/13	1
Writing Project Proposal	01/03/13	04/03/13	2
Supervisor's review of Project Proposal	04/03/13	04/03/13	1
Research on Related Work and Writting Interim Report	04/03/13	19/03/13	12
Discussion with the Supervisor Concerning Interim Report	11/03/13	11/03/13	1
Further Work On The Interim Report	12/03/13	15/03/13	4
Workshop 3: Literature Searching	18/03/13	18/03/13	1
Further Work On Interim Report	19/03/13	21/03/13	3
Supervisor's Review of Interim Report	22/03/13	22/03/13	1
Planning of Artefact Design and Brief Meeting with the Supervisor	25/03/13	28/03/13	4
Outline of Thesis Table of Content	28/03/13	02/04/13	4
Discussion With The Supervisor on the Artefact	01/04/13	01/04/13	1
Further Research Regarding the Artifact	02/04/13	05/04/13	4
Meeting With The Supervisor	08/02/13	08/02/13	1
Finalising The Interim Report	09/04/13	12/04/13	4
Discussion With The Supervisor	15/04/13	15/04/13	1
Thesis Writing plan	16/04/13	18/04/13	3
Submission of Interim Report	19/04/13	19/04/13	1
Drafting The Artifact Structure	20/02/13	21/02/13	2
Presentating Artefact Structure to the Supervisor	22/04/13	22/04/13	1
Thesis Writting	23/04/13	26/04/13	4
Meeting With The Supervosor	29/04/13	29/04/13	1
Further Work On The Artefact	30/05/13	05/06/13	5
Discussing The Artefact With The Supervisor	06/05/13	06/05/13	1
Abstract and Further Writting	07/05/13	13/05/13	5
Artefact Implementation	14/05/13	23/05/13	8
Supervisor's Review of Artifact and the Abstract	20/05/13	20/05/13	1
Effecting Neccessary Corrections	21/05/13	21/05/13	1
Project Poster	22/05/13	22/05/13	1
Workshop 4: Thesis Submission and Viva	23/05/13	23/05/13	1
Submission of Final Report	24/05/13	24/05/13	1
Viva Preparation	27/05/13	27/05/13	1
Viva Presentation	27/05/13	07/06/13	10

APPENDIX D

PROJECT POSTER

University of Bedfordshire

AN ACCESS CONTROL SYSTEM TO IMPROVE SECURITY AMONGST RANDOMLY ASSOCIATED NODES IN BYOD NETWORK.

Student: FRANCIS NWEBONYI NWEBONYI **Course:** Msc. Computer Security and Forensics.
Reg No: 1029282 **Supervisor:** Dr. Gregory Epiphaniou

Introduction

Bring Your Own Device (BYOD) is a concept that allow employees to bring personally owned mobile devices for official work. It has gained much popularity among enterprises because of the tremendous growth in the number of mobile devices available in the market today. The concept is bringing a shift from the usual approach where concerned organisations/enterprises usually own and manage the devices used for official tasks; keeping adequate watch on their security status. BYOD shifts the ownership of these devices to the employees, and introduces mobile devices instead of the relatively stationary ones. Although with numerous advantages including reduced cost, employee satisfaction, increased productivity, among others, some security limitations are also introduced owing to its highly dynamic nature. The introduced security concerns falls beyond the scope of the traditional access control systems that the organisations are used to. This work therefore studies similar dynamic environments, relating to how their security challenges are addressed, as a bases to propose an algorithm for enhancing the security of BYOD via access control.

Statement of The Problem

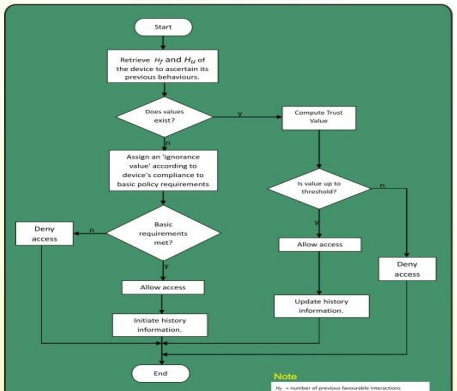
BYOD as a type of pervasive environment involves unavoidable mutual collaborations of mobile devices, leading to more security issues than those experienced in traditional networks . The IT department of the organisations involved cannot answer questions concerning the security state of the interacting nodes at any point, because the ownership of the devices have been lost to the employees. The fact that mobile devices easily collaborate with other external devices, makes it exposed to higher risk of threats, and thus more difficult to be securely incorporated into a network. Access control plays key role in addressing many security issues, but in the case of BYOD, the usual traditional access control systems used in organisations cannot adequately fend for its dynamic security needs. This project studies existing access control systems and the security approaches currently used in other pervasive environments, and matching them accordingly to derive an access control algorithm for increasing the security of BYOD network.

Aim and Objectives

The aim of this work is to derive an algorithm for a Device Aware Access Control (DAAC) system that increases the security of BYOD networks based on trust. The algorithm is to ascertain the trust worthiness of interacting nodes beforehand via trust value computation, which is then used for access permission decision. This is geared towards securing the network resources by dictating and dropping malicious (non trustworthy) node(s) out of the network to prevent it from causing security breaches. The following objectives shall be achieved;

- Extensive review of BYOD concepts, existing access control and trust models.
- Deriving suitable parameters for acquiring and monitoring interaction history of the randomly associated nodes.
- Deriving a mathematical method of computing trust value of nodes, which also portray their expected behaviour if allowed access to the network.
- Proposing a trust based algorithm for screening out malicious nodes in a BYOD network, as a way of increasing its security. The past interactions of each randomly associated node will be used to calculate its subsequent security behaviour using the principles of probability theory.

Flowchart of Proposed Algorithm



Summarised Pseudo Code of flowchart

```
START
GET Hf and Hu
numOfFaint = Hf
numOfUnint = Hu
IF ((numOfFaint == 0) & (numOfUnint == 0))
        IF (Device meet company policy)
                Tv = Tmin
                Allow Access
                Initiate History Information
        ELSE
                Deny Access
ELSE
        IF ((ComputeTrust(numOfFaint, numOfUnint)) < Tmin )
                Deny Access
        ELSE
                Allow Access
                Update History Information
END IF
ComputeTrust(Hf , Hu) //Function to compute trust
trust = Tv = E(p) = (Hf + 1)/(Hf + Hu + 2)
RETURN (trust)
END
```

Mathematical Expression

- For first-time devices:

An ignorance value expressed as $R \in \{0, T_{min}\}$ is usually assigned to first time devices which has no previous interaction history with the network, as their trust value (T_v). The value to be assigned will be based on compliance with the organisational policies on; device registration, approved device type, and operating system version. It is further compared with the trust threshold to determine a pass or a drop.

$$T_v = \begin{cases} T_{min} \\ 0 \end{cases} \quad 0 \le T_v \le T_{min}$$

$T_v = T_{min}$ ⟶ Allow Access

$T_v < T_{min}$ ⟶ Deny Access

- Returning Devices

In this case the trust value is calculated with the following equation

$$T_v = E(p) = \frac{H_f + 1}{H_f + H_u + 2}$$

$$0 \le E(P) \le 1$$

Where H_f = the number of favourable interaction for a given device,

H_u = the number of unfavourable interaction of same device, and

T_v = the trust value of the devices

$E(p)$ = expected probability of nodes' behaviour (favourable or unfavourable).

Result and Analysis

Tables 1 and 2 represents a sample calculation of our algorithm using the stated mathematical expression.

Table 1: Interaction History for device A with increasing favourable behaviour.

Number of previous interaction	Number of previous unfavourable interactions ( )	Number of previous favourable interactions ( )	Calculated trust value ( )	Access Decision
2	1	1	0.5	Pass
10	1	9	0.833	Pass
20	1	19	0.909	Pass
30	1	29	0.937	Pass
40	1	39	0.952	Pass
50	1	49	0.961	Pass
60	1	59	0.967	Pass
70	1	69	0.972	Pass
80	1	79	0.975	Pass
90	1	89	0.978	Pass
100	1	99	0.980	Pass

Table 2: Interaction History for device B with increasing unfavourable (malicious) behaviour

Number of previous interaction	Number of previous unfavourable interactions ( )	Number of previous favourable interactions ( )	Calculated trust value (T_b)	Access Decision
2	1	1	0.5	Pass
10	9	1	0.1666	Deny
20	19	1	0.0909	Deny
30	29	1	0.0652	Deny
40	39	1	0.0476	Deny
50	49	1	0.0384	Deny
60	59	1	0.0322	Deny
70	69	1	0.0277	Deny
80	79	1	0.0243	Deny
90	89	1	0.0217	Deny
100	99	1	0.0196	Deny

Figure 1 presents the graphical representation of the computation of tables 1 and 2; demonstrating that trusted (potentially safe) devices were allow to access the network while the untrustworthy (potentially malicious) ones were dropped.

Figure 1: Effects of Favourable (T_{fv}) and Unfavourable (T_{fu}) interactions on Trust Value (T_v) and Access Decision.

Comparison with existing approach

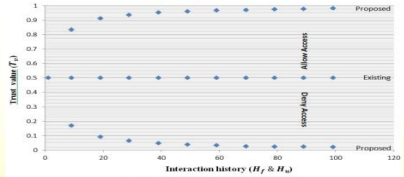


Figure 2: A Comparison with the existing system

The existing security framework as presented in (Armando, Gabriele & Merlo, 2013) acted indifferently to the activities of the devices after the initial security policy is met, thus allowing malicious nodes to repeatedly access the network. Our approach however considered the high level of dynamism among the randomly associated nodes in BYOD network, and keeps a watch on them, to block off potentially malicious ones, and allow only the potentially safe ones to gain access; thus enhancing the security of the network.

Conclusion

This work has adequately explored the concepts of BYOD, its advantages and security limitations. Trust have also been thoroughly discussed, including its related applications. We have also done justice to various access control models, highlighting their strengths and weaknesses as a bases for our approach. Finally, the proposed algorithm have employed the concept of trust on the access control system of BYOD in a manner that allow for adequate dynamism and enhanced security of the network.